UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/972,226	10/04/2001	Vadim Lander	063170.6963(20000430)	4394

5073 7590 06/07/2006	EXAMINER
BAKER BOTTS L.L.P.	SHIFERAW, ELENI A

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 06/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

		Application No.	Applicant(s)
Office Action Summary		09/972,226	LANDER, VADIM
		Examiner	Art Unit	
		Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 March 2006*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   Applicant's arguments with respect to pending claims 1-30 filed on 03/27/2006 have been

fully considered but they are not persuasive. The examiner would like to point out that this action

is made final (MPEP 706.07a).

Response to Arguments

2.   Applicant argues that:

The applicant's first argument concerns, with 102 rejections, Saito failure to disclose

"searching for information relating to a user in a user in a repository of user information, the

searching based at least partially on said user request and login identity supplied by said user"

as recited in claims 1 and 28 or "providing identifying data to said network" as recited in claim

12 or "accessing a repository containing a plurality of unique universal user identifiers, each of

said unique universal user identifiers being unique to a user" as recited in claim 18 or "a first

software tool operable to receive user login information, access said repository" as recited in

claim 23 and *"retrieving a unique universal user identifier representing said user upon locating*

said information" as recited in claims 1, 12, 18, 23, and 28. The examiner respectfully disagrees

with the applicant's contentions and would like to draw the Applicant's attention to col. 2 lines

28-39 and col. 5 lines 51-56 wherein Saito discloses ... **the client transmitting a *user ID and a***

***password* to the application server to initially make a service request, in single sign-on**

method, and the application server transferring the user ID and the password to the

integrated authentication server. In that case, the integrated authentication server checks

the user for the right to access the application server and if valid, the integration

authentication server prepares an *integral certificate (unique universal user identifier)* and

Saito on col. 5 also describes, creating an *integrated certificate* through conventional log-in

effected by *inputting a user ID and a password* and thereafter, each time that the server

process shifts from one to another, the client transmits the integrated certificate to a

particular application server, thereby permitting a single sign-on. It is clear that the

integrated authentication sever repository contains plurality of different unique integrated

certificates to identify different users and integrated certificate is retrieved for users based on

user request containing user ID and password that users provide to integrated authentication

server to access multiple resources.

As per Applicant's concerning, 103 rejection, failure to teach same limitations argued as

above, the Examiner would like to refer back to col. 6 lines 19-51, wherein Cohen teaches

receiving user request to access target application on a target resource in a distributed computer

enterprise, the user information is searched, and passwords/keys and the target logon information

are retrieved from repository (PKM and/or CIM) based on the user request to access resources.

The logon coordinator then uses the retrieved passwords/keys and the target login information to

sign-on to various target systems and application resources.

Wood discloses in a networked information environment having multiple resources, the

network, generating a unique universal user identifier or "unique session identifier" and

retrieving and/or storing the generated unique session cookie identifier on the client browser to

indicate the user is authenticated and allowing single sign-on authenticated access to multiple

resources (Wood col. 24, lines 5-4, col. 3 lines 2-6, and 45-53, col. 11 lines 60-67, col. 12 lines

52-col. 13 lines 36 and col. 22 lines 20-40). Unique session identifier is a unique session token

which may be any data supplied to the client entity for use in uniquely identifying an associated

session in communication of multiple resources in a method of single sign-on. Unique session

identifier is also employed to facilitate session continuity and to allow the security architecture to

associate prior authentication of login credentials with an incoming access request. Session

tokens are issued to client entities as part of an interaction with the security architecture and are

thereafter presented with access requests (claim 2 and col. 8 lines 54-col. 9 lines 11).

Johnson discloses a method that allows a single sign-on authentication of customers in a

multi-vendor e-commerce environment and to methods and systems for directory authentication

of electronic bank drafts (col. 1 lines 13-17), authenticator server has a **repository (master list)**

that holds unique user identifiers that is uniquely generated for users based on user's

information, **unique user identifier is retrieved from the master list repository** and compared

with request identifier whenever the user requests an access to multiple vendor's and access to

multiple resources is granted or denied based on authentication (col. 10 lines 19-27, col. 3 lines

28-63, and col. 6 lines 61-67). Accordingly, claims 1-30 stand rejected.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

4.   Claims 12-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al.

(Cohen, Patent No.: US 6,178,511 B1) in view of Wood et al. (Wood, Patent No.: US 6,609,198

B1) and Johnson US 6,898,577 B1.

As per claim 12, Cohen teaches an electronic device in communication with a network, a method

for a user to access a plurality of resources having different authorization requirements, the

method comprising:

        accessing, via an electronic device, network comprising a plurality of resources (Cohen

claim 1);

        providing identifying data to said network (Cohen Col. 6 lines 19-37);

        retrieving a unique user identifier corresponding to said user from repository of

unique user identifiers (Cohen claim 9, Col. 6 lines 19-col. 7 lines 20, col. 2 lines 33-41and col. 5

lines 16-44);

        storing said unique user identifier on a storage device, said unique

user identifier indicating said user is authenticated (Cohen Col. 2 lines 33-4, and col. 2 lines 60-

col. 7 lines 7); and

        accessing one of said plurality of resources, wherein said unique user identifier is

transmitted to said one of said plurality of resources to identify said user such that said user can

access authorized resources without providing additional identifying information (Cohen Col. 2

lines 33-41, and abstract) and said user is denied access to unauthorized resources (Cohen Col.

10 lines 18-38).

        Cohen fails to explicitly teach unique universal user identifier.

However **Wood** teaches in a networked information environment having multiple

resources, the network, generating a unique session cookie identifier **that is used to identify a**

unique user's session and storing the generated unique session cookie identifier on the client

browser to indicate the user is authenticated and allow single sign-on authenticated access to

multiple resources (Wood col. 14 lines 5-14, col. 3 lines 2-6, and 45-53, col. 11 lines 60-67, col.

12 lines 52-col. 13 lines 36 and col. 22 lines 20-40).

Therefore it would have been obvious to one having ordinary skill in the art at the time of

the invention was made to employ the teachings of Wood within the system of Cohen because

they are analogous in single sign-on (Wood abstract). One skilled in the art would have been

motivated to incorporate the teachings of Wood within the system of Cohen because it would

enhance security by generating a unique user identifier to access plurality of resources in a single

sign on method (col. 14 lines 5-14, col. 3 lines 2-6, and 45-53, and col. 11 lines 60-67).

The combination of Cohen and Wood teach all the subject matter as described above.

And Wood discloses providing a method of single sign-on multi-level authentication access to a

*user application/browser upon user request to resources/enterprise applications by **assigning***

and retrieving a unique universal session identifier that is given to identify a particular user

for session in order to access enterprise resources (Wood col. 2 lines 27-col. 3 lines 53). Cohen

and Wood fail to disclose the retrieved unique universal session identifier representing said user

*upon locating said information of the user **is from the repository of user information**.*

However Johnson discloses a method that allows a single sign-on authentication of

customers in a multi-vendor e-commerce environment and to methods and systems for directory

authentication of electronic bank drafts (col. 1 lines 13-17), authenticator server has a

repository (master list) that holds unique user identifiers that is uniquely generated for users

based on user's information, unique user identifier is retrieved from the master list repository

and compared with request identifier whenever the user requests an access to multiple vendor's

and access to multiple resources is granted or denied based on authentication (col. 10 lines 19-

27, col. 3 lines 28-63, and col. 6 lines 61-67).

Therefore it would have been obvious to one having ordinary skill in the art at the time of

the invention was made to employ the teachings of Johnson within the combination of Cohen

and Wood because they are analogous in single sign-on (abstract). One would have been

motivated to incorporate the teachings of retrieving a unique user identifier from repository of

user information within the combination system, to efficiently provide access to multiple

resources avoid re-authentication of a user.

As per claim 13, Cohen, Wood, and Johnson teach all the subject matter as described above. In

addition, the combination of the prior art record teach the method, further comprising providing a

key to retrieve an authorization datum associated with one of said plurality of unique user

identifiers matching said unique universal user identifier from one of said plurality of resources

(Cohen Col. 6 lines 19-59, and Wood col. 14 lines 5-14, col. 3 lines 2-6, and 45-53, and col. 11

lines 60-67).

As per claim 14, Cohen, Wood, and Johnson teach all the subject matter as described above. In

addition, the combination of the prior art record teach the method, further comprising:

       registering said user with said network (Cohen Col. 5 lines 16-58);

generating said unique universal user identifier for said user (Cohen Col. 5 lines 16-58,

and Wood col. 14 lines 5-14, col. 3 lines 2-6, and 45-53, col. 11 lines 60-67, col. 12 lines 52-col.

13 lines 36 and col. 22 lines 20-40); and

inserting said unique universal user identifier in at least one of said plurality

of user identifiers (Cohen Col. 5 lines 16-58, and Wood col. 14 lines 5-14, col. 3 lines 2-6, and

45-53, col. 11 lines 60-67, col. 12 lines 52-col. 13 lines 36 and col. 22 lines 20-40).

As per claim 15, Cohen, Wood, and Johnson teach all the subject matter as described above. In

addition Cohen teaches the method, wherein providing identifying data to said network

comprises supplying at least one of a login name, a password, and a digital certificate (Cohen

Col. 5 lines 45-53; a user supplying a password and ID).

As per claim 16, Cohen, Wood, and Johnson teach all the subject matter as described above. In

addition Cohen teaches the method, wherein providing identifying data to said network

comprises providing user credentials (Cohen Col. 5 lines 45-53; a user supplying a password and

ID, target name, and user preferences).

5.   Claims 1-4, 6-11, and 18-30 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Cohen et al. (Cohen, Patent No.: US 6,178,511 B1) in view of Weissman (Pub. No.: US

2002/0161901 A1), Wood et al. (Wood, Patent No.: US 6,609,198 B1) and Johnson US

6,898,577 B1.

As per claim 1, Cohen teaches a method for authenticating and authorizing a user of an

electronic device in communication with a network, (Cohen Abstract), comprising:

receiving a user request from a user of an electronic device in communication with a

network (Cohen Col. 6 lines 60-col. 7 lines 20, and fig. 1 No. 20 and No. 14,16, & 18; the server

(20) receiving a user request from device (14));

searching for information relating to said user in a repository of user information,

said searching based at least partially on said user request and a login identity supplied by said

user (Cohen Col. 6 lines 19-col. 7 lines 20, and col. 5 lines 16-44, the server searches the

database according to the user's request to sign-on a user to various target systems);

retrieving a user identifier representing said user upon locating said information of said

user (Cohen Col. 6 lines 19-col. 7 lines 20, col. 2 lines 33-41and col. 5 lines 16-44); and

receiving an authorization datum associated with said user, based at least partially on said

user identifier, from said resource (Cohen Abstract, and col. 2 lines 33-41; a target resource in a

distributed computer enterprise is accessed by an authorized user);

Cohen does not explicitly teach:

storing at least said user identifier in a data packet; and

sending said data packet to a storage device such that said data packet is

transmittable to electronic devices in communication with said network when said user attempts

to access a resource within said network;

However **Weissman** discloses a single logon system for logging onto multiple

server computers by storing at least said user identifier in a data packet (Weissman Claim 1,

claim 15, and claim 28);

sending said data packet to a storage device such that said data packet is

transmittable to electronic devices in communication with said network when said user attempts

to access a resource within said network (Weissman Page 6 par. 0032, and page 7 par. 0036);

Therefore it would have been obvious to one havening ordinary skill in the art at the time

the invention was made to employ the teachings of Weissman within the system of Cohen

because it would allow to automatically logon a user to multiple web sites or resources without

signing more than one time (using single logon) (Weissman Page 3 par. 0022).

Cohen and Weissman fail to explicitly teach unique universal user identifier.

However **Wood** teaches in a networked information environment having multiple

resources, the network, generating a unique session cookie identifier and storing the generated

unique session cookie identifier on the client browser to indicate the user is authenticated and

allow single sign-on authenticated access to multiple resources (Wood col. 14 lines 5-14, col. 3

lines 2-6, and 45-53, col. 11 lines 60-67, col. 12 lines 52-col. 13 lines 36 and col. 22 lines 20-40).

Therefore it would have been obvious to one having ordinary skill in the art at the time of

the invention was made to employ the teachings of Wood within the system of Cohen and

Weissman because they are analogous in single sign-on (Wood abstract). One skilled in the art

would have been motivated to incorporate the teachings of Wood within the system of Cohen

and Weissman because it would enhance security by generating a unique user identifier to access

plurality of resources in a single sign on method (col. 14 lines 5-14, col. 3 lines 2-6, and 45-53,

and col. 11 lines 60-67).

The combination of Cohen, Weissman and Wood teach all the subject matter as described

above. And Wood discloses providing a method of single sign-on multi-level authentication

access to a user application/browser upon user request to resources/enterprise applications by

assigning and retrieving a unique universal session identifier that is given to identify a

particular user for session *in order to access enterprise resources (Wood col. 2 lines 27-col. 3*

lines 53). Cohen, Weissman and Wood fail to disclose the retrieved unique universal session

*identifier representing said user upon locating said information of the user **is from the***

repository of user information.

However Johnson discloses a method that allows a single sign-on authentication of

customers in a multi-vendor e-commerce environment and to methods and systems for directory

authentication of electronic bank drafts (col. 1 lines 13-17), authenticator server has a

repository (master list) that holds unique user identifiers *that is uniquely generated for users*

*based on user's information, **unique user identifier is retrieved from the master list repository***

and compared with request identifier whenever the user requests an access to multiple vendor's

and access to multiple resources is granted or denied based on authentication (col. 10 lines 19-

27, col. 3 lines 28-63, and col. 6 lines 61-67).

Therefore it would have been obvious to one having ordinary skill in the art at the time of

the invention was made to employ the teachings of Johnson within the combination of Cohen,

Weissman and Wood because they are analogous in single sign-on (abstract). One would have

been motivated to incorporate the teachings of retrieving a unique user identifier from repository

of user information within the combination system, to efficiently provide access to multiple

resources avoid re-authentication of a user.

As per claim 18, Cohen teaches a method for user authentication and authorization, comprising:

a plurality of user identifiers, each of said unique universal user identifiers being unique

to a user (Cohen Col. 6 lines 19-37);

retrieving one of said user identifier (Cohen Col. 6 lines 19-45); and

Cohen does not explicitly teach:

storing said user identifier in a data packet readable by an electronic device;

transmitting said data packet to a storage device coupled to said electronic

device; and

making said data packet available to a resource configured within an enterprise

network to authorize said user.

However **Weissman** discloses a single logon system for logging onto multiple

server computers by storing said user identifier in a data packet readable by an electronic device

(Weissman Claim 1, claim 15, and claim 28);

transmitting said data packet to a storage device coupled to said electronic device

(Weissman Page 6 par. 0032, and page 7 par. 0036); and

making said data packet available to a resource configured within an enterprise

network to authorize said user (Weissman Page 6 par. 0032, page 7 par. 0036, and abstract).

Therefore it would have been obvious to one havening ordinary skill in the art at the time

the invention was made to employ the teachings of Weissman within the system of Cohen

because it would allow to automatically logon a user to multiple web sites or resources without

signing more than one time (using single logon) (Weissman Page 3 par. 0022).

Cohen and Weissman fail to explicitly teach unique universal user identifier.

However **Wood** teaches in a networked information environment having multiple

resources, the network, generating a unique session cookie identifier and storing the generated

unique session cookie identifier on the client browser to indicate the user is authenticated and

allow single sign-on authenticated access to multiple resources (Wood col. 14 lines 5-14, col. 3

lines 2-6, and 45-53, col. 11 lines 60-67, col. 12 lines 52-col. 13 lines 36 and col. 22 lines 20-40).

Therefore it would have been obvious to one having ordinary skill in the art at the time of

the invention was made to employ the teachings of Wood within the system of Cohen and

Weissman because they are analogous in single sign-on (Wood abstract). One skilled in the art

would have been motivated to incorporate the teachings of Wood within the system of Cohen

and Weissman because it would enhance security by generating a unique user identifier to access

plurality of resources in a single sign on method (col. 14 lines 5-14, col. 3 lines 2-6, and 45-53,

and col. 11 lines 60-67).

The combination of Cohen, Weissman and Wood teach all the subject matter as described

above. And Wood discloses providing a method of single sign-on multi-level authentication

access to a user application/browser upon user request to resources/enterprise applications by

assigning and retrieving a unique universal session identifier that is given to identify a

particular user for session *in order to access enterprise resources (Wood col. 2 lines 27-col. 3*

lines 53). Cohen, Weissman and Wood fail to disclose the retrieved unique universal session

*identifier representing said user upon locating said information of the user **is from the***

repository of user information.

However Johnson discloses a method that allows a single sign-on authentication of

customers in a multi-vendor e-commerce environment and to methods and systems for directory

authentication of electronic bank drafts (col. 1 lines 13-17), authenticator server has a

repository (master list) that holds unique user identifiers that is uniquely generated for users

based on user's information, unique user identifier is retrieved from the master list repository

and compared with request identifier whenever the user requests an access to multiple vendor's

and access to multiple resources is granted or denied based on authentication (col. 10 lines 19-

27, col. 3 lines 28-63, and col. 6 lines 61-67).

Therefore it would have been obvious to one having ordinary skill in the art at the time of

the invention was made to employ the teachings of Johnson within the combination of Cohen,

Weissman and Wood because they are analogous in single sign-on (abstract). One would have

been motivated to incorporate the teachings of retrieving a unique user identifier from repository

of user information within the combination system, to efficiently provide access to multiple

resources avoid re-authentication of a user.

As per claim 23, Cohen teaches a network of electronic devices suitable for implementing a

system for user authentication and authorization, comprising:

a repository containing a plurality of user identifiers, each user identifier being

unique to a user (Cohen Col. 5 lines 16-40, col. 6 lines 19-37, and Col. 9 lines 47-67);

a first software tool operable to receive user login information, access said

repository, retrieve a user identifier relating to said user (Cohen Col. 6 lines 19-45), and

Cohen does not explicitly teach:

transmit said user identifier to an electronic storage device suitable for storing said user

identifier in a data packet for transmission to resources within a network; and

a second software tool suitable for receiving said data packet and locating

authorization datum of said user.

However **Weissman** discloses a single logon system for logging onto multiple server

computers by transmitting any such user identifier to an electronic storage device suitable for

storing said user identifier in a data packet for transmission to resources within said network

(Weissman Page 6 par. 0032, claim 3, and page 7 par. 0036); and

a second software tool suitable for receiving said data packet and locating

authorization datum of said user (Weissman Page 6 par. 0032, fig. 3 No. 310, and page 7 par.

0036).

Therefore it would have been obvious to one havening ordinary skill in the art at the time

the invention was made to employ the teachings of Weissman within the system of Cohen

because it would allow to automatically logon a user to multiple web sites or resources without

signing more than one time (using single logon) (Weissman Page 3 par. 0022).

Cohen and Weissman fail to explicitly teach unique universal user identifier.

However **Wood** teaches in a networked information environment having multiple

resources, the network, generating a unique session cookie identifier and storing the generated

unique session cookie identifier on the client browser to indicate the user is authenticated and

allow single sign-on authenticated access to multiple resources (Wood col. 14 lines 5-14, col. 3

lines 2-6, and 45-53, col. 11 lines 60-67, col. 12 lines 52-col. 13 lines 36 and col. 22 lines 20-40).

Therefore it would have been obvious to one having ordinary skill in the art at the time of

the invention was made to employ the teachings of Wood within the system of Cohen and

Weissman because they are analogous in single sign-on (Wood abstract). One skilled in the art

would have been motivated to incorporate the teachings of Wood within the system of Cohen

and Weissman because it would enhance security by generating a unique user identifier to access

plurality of resources in a single sign on method (col. 14 lines 5-14, col. 3 lines 2-6, and 45-53,

and col. 11 lines 60-67).

The combination of Cohen, Weissman and Wood teach all the subject matter as described

above. And Wood discloses providing a method of single sign-on multi-level authentication

access to a user application/browser upon user request to resources/enterprise applications by

assigning and retrieving a unique universal session identifier that is given to identify a

particular user for session *in order to access enterprise resources (Wood col. 2 lines 27-col. 3*

lines 53). Cohen, Weissman and Wood fail to disclose the retrieved unique universal session

identifier representing said user upon locating said information of the user ***is from the***

repository of user information.

However Johnson discloses a method that allows a single sign-on authentication of

customers in a multi-vendor e-commerce environment and to methods and systems for directory

authentication of electronic bank drafts (col. 1 lines 13-17), authenticator server has a

repository (master list) that holds unique user identifiers *that is uniquely generated for users*

based on user's information, ***unique user identifier is retrieved from the master list repository***

and compared with request identifier whenever the user requests an access to multiple vendor's

and access to multiple resources is granted or denied based on authentication (col. 10 lines 19-

27, col. 3 lines 28-63, and col. 6 lines 61-67).

Therefore it would have been obvious to one having ordinary skill in the art at the time of

the invention was made to employ the teachings of Johnson within the combination of Cohen,

Weissman and Wood because they are analogous in single sign-on (abstract). One would have

been motivated to incorporate the teachings of retrieving a unique user identifier from repository

of user information within the combination system, to efficiently provide access to multiple

resources avoid re-authentication of a user.

As per claim 28, Cohen teaches a computer readable medium encoded with logic operable, when

executed on a computer processor, to perform the steps comprising:

receiving a user request from a user of an electronic device (Cohen Col. 6 lines 60-col. 7

lines 20, and fig. 1 No. 20 and No. 14,16, & 18; the server (20) receiving a user request device

(14));

searching for a user credential corresponding to said user in an authentication database

(Cohen Col. 6 lines 19-col. 7 lines 20, and col. 5 lines 16-44, the server searches the database

according to the user's request to sign-on a user to various target systems);

locating said user credential in said authentication database (Cohen Col. 6 lines 19-col. 7

lines 20, and col. 5 lines 16-44);

retrieving a universal identifier representing said user upon locating said

user credential (Cohen Col. 6 lines 19-col. 7 lines 20, col. 2 lines 33-41and col. 5 lines 16-44);

Cohen does not explicitly teach:

packaging said universal identifier in a data packet; and

transmitting said data packet to said electronic device such that said data packet is

transmittable to electronic devices in communication with a network when said user attempts to

access a resource within said network such that said user can access authorized resources without

providing additional identifying information.

However **Weissman** discloses a single logon system for logging onto multiple server

computers by packaging said universal identifier in a data packet (Weissman Page 6 par. 0032,

claim 3, and page 7 par. 0036); and

transmitting said data packet to said electronic device such that said data packet is

transmittable to electronic devices in communication with a network when said user attempts to

access a resource within said network such that said user can access authorized resources without

providing additional identifying information (Weissman Page 6 par. 0032, fig. 3 No. 310, and

page 7 par. 0036).

Therefore it would have been obvious to one havening ordinary skill in the art at the time

the invention was made to employ the teachings of Weissman within the system of Cohen

because it would allow to automatically logon a user to multiple web sites or resources without

signing more than one time (using single logon) (Weissman Page 3 par. 0022).

Cohen and Weissman fail to explicitly teach unique universal user identifier.

However **Wood** teaches in a networked information environment having multiple

resources, the network, generating a unique session cookie identifier and storing the generated

unique session cookie identifier on the client browser to indicate the user is authenticated and

allow single sign-on authenticated access to multiple resources (Wood col. 14 lines 5-14, col. 3

lines 2-6, and 45-53, col. 11 lines 60-67, col. 12 lines 52-col. 13 lines 36 and col. 22 lines 20-40).

Therefore it would have been obvious to one having ordinary skill in the art at the time of

the invention was made to employ the teachings of Wood within the system of Cohen and

Weissman because they are analogous in single sign-on (Wood abstract). One skilled in the art

would have been motivated to incorporate the teachings of Wood within the system of Cohen

and Weissman because it would enhance security by generating a unique user identifier to access

plurality of resources in a single sign on method (col. 14 lines 5-14, col. 3 lines 2-6, and 45-53,

and col. 11 lines 60-67).

The combination of Cohen, Weissman and Wood teach all the subject matter as described

above. And Wood discloses providing a method of single sign-on multi-level authentication

access to a user application/browser upon user request to resources/enterprise applications by

assigning and retrieving a unique universal session identifier that is given to identify a

***particular user for session** in order to access enterprise resources (Wood col. 2 lines 27-col. 3*

lines 53). Cohen and Wood fail to disclose the retrieved unique universal session identifier

*representing said user upon locating said information of the user **is from the repository of user***

***information**.*

However Johnson discloses a method that allows a single sign-on authentication of

customers in a multi-vendor e-commerce environment and to methods and systems for directory

authentication of electronic bank drafts (col. 1 lines 13-17), authenticator server has a

***repository (master list) that holds unique user identifiers** that is uniquely generated for users*

*based on user's information, **unique user identifier is retrieved from the master list repository***

and compared with request identifier whenever the user requests an access to multiple vendor's

and access to multiple resources is granted or denied based on authentication (col. 10 lines 19-

27, col. 3 lines 28-63, and col. 6 lines 61-67).

Therefore it would have been obvious to one having ordinary skill in the art at the time of

the invention was made to employ the teachings of Johnson within the combination of Cohen,

Weissman and Wood because they are analogous in single sign-on (abstract). One would have

been motivated to incorporate the teachings of retrieving a unique user identifier from repository

of user information within the combination system, to efficiently provide access to multiple

resources avoid re-authentication of a user.

As per claim 2, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described

above. In addition Cohen teaches the method, wherein receiving a user request comprises

receiving a login name from said user (Cohen Col. 5 lines 45-58, and col. 2 lines 33-41).

As per claim 3, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described

above. In addition Cohen teaches the method, further comprising:

registering said user with said network (Cohen Col. 5 lines 16-58);

generating said user identifier relating to said user (Cohen Col. 5 lines 16-58);

inserting said user identifier in said repository of user information (Cohen Col. 5 lines 16-

58); and

populating a plurality of repositories containing authorization data with said user

identifier (Cohen Col. 5 lines 16-col. 6 lines 45).

As per claim 4, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described above. In addition Cohen teaches the method, further comprising receiving a security identity from said user (Cohen Col. 6 lines 19-37).

As per claim 5, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described above. In addition Wood disclose the method further comprising receiving a digital certificate from sid user (Wood col. 6 lines 17-23).

As per claim 6, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described above. In addition Cohen teaches the method, further comprising indicating a result to said user regarding permitted access to said network (Cohen Col. 6 lines 8-37, and col. 10 lines 15-38).

As per claim 7, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described above. In addition Cohen teaches the method, further comprising requesting a user credential of said user (Cohen Col. 6 lines 8-37).

As per claim 8, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described above. In addition Weissman teaches the method, wherein sending said data packet to a storage device comprises sending said data packet to a user electronic device supporting said storage device (Weissman Page 6 par. 0032, fig. 3 No. 310, and page 7 par. 0036; data structure is sent to user's web). The rational for combining are the same as claim 1 above.

As per claim 9, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described above. In addition Weissman teaches the method, further comprising storing information in addition to said unique universal user identifier in said data packet (Weissman Page 6 par. 0032, fig. 3 No. 310, and page 7 par. 0036; the user computer receives the cookies and stores the cookies on the user's computer). The rational for combining are the same as claim 1 above.

As per claim 10, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described above. In addition Weissman teaches the method, wherein sending said data packet to a storage device comprises transmitting a cookie to said user electronic device enabling an identity of said user to be automatically recognized when said cookie is transmitted to said resource within said network (Weissman Page 6 par. 0032, fig. 3 No. 310, and page 7 par. 0036; the user computer receives the cookies and stores the cookies on the user's computer to be automatically recognized). The rational for combining are the same as claim 1 above.

As per claim 11, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described above. In addition Cohen teaches the method, further comprising encrypting said data packet (Cohen Col. 6 lines 19-37).

As per claim 17, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described above. In addition Wood teaches the method, wherein providing identifying data to said network comprises providing a digital certificate (Wood col. 6 lines 17-23)

As per claim 19, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described above. In addition Weissman teaches the method, wherein storing said unique universal user identifier comprises packaging said unique universal user identifier in a cookie suitable for storage on at least one of a user electronic device and a user proxy electronic device (Weissman Page 6 par. 0032, fig. 3 No. 310, and page 7 par. 0036; the user computer receives the cookies and stores the cookies on the user's computer to be automatically recognized). The rational for combining are the same as claim 1 above.

As per claim 20, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described above. In addition Cohen teaches the method, further comprising employing a software program to access a network reading said storage device (Cohen Col. 5 lines 16-col. 46).

As per claim 21, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described above. In addition Weissman teaches the method, further comprising employing a web browser employed to access a network reading said storage device (Weissman Page 7 par. 0036). The rational for combining are the same as claim 18 above.

As per claim 22, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described above. In addition Cohen teaches the method, further comprising:

delivering said data packet to said resource configured within said enterprise

network;

extracting said unique universal user identifier from said data packet (Cohen Col. 6 lines

19-45);

accessing a repository containing a plurality of user entitlement data (Cohen Col. 5 lines

16-col.6 lines 45); and

retrieving a user-specific entitlement from said repository containing said

plurality of user entitlement data using said unique universal user identifier to locate said user-

specific entitlement (Cohen Col. 5 lines 16-col.6 lines 45; user is authenticated and entitlement is

retrieved to the resource and access to the resource is allowed).

As per claim 24, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described

above. In addition Cohen teaches the system, wherein said electronic storage device is readable

by a software program suitable for accessing said network (Cohen Col. 3 lines 60-col. 4 lines

21).

As per claim 25, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described

above. In addition Weissman teaches the system, wherein said software program is a web

browser (Weissman Page 7 par. 0036, and abstract).

As per claim 26, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described

above. In addition Cohen teaches the system, wherein said electronic storage device is a resource

configured within said network (Cohen Abstract; target resources).

As per claim 27, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described above. In addition Cohen teaches the system, further comprising a repository containing authorization data, said repository containing authentication data accessible using said unique universal user identifier as a key to retrieve a user-specific entitlement associated with said user (Cohen Col. 5 lines 16-col. 6 lines 37).

As per claim 29, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described above. In addition Cohen teaches the computer readable medium, further operable, when executed on a computer processor, to perform the steps comprising:

transmitting said data packet to said resource within said network (Wood col. 11 lines 60-67);

accessing a repository containing a plurality of user identifiers using said packaged unique universal user identifier in a search operation (Cohen Col. 6 lines 19-col. 7 lines 20, and col. 5 lines 16-44, the server searches the database according to the user's request to sign-on a user to various target systems); and

retrieving a user-specific entitlement from said repository containing a plurality of unique universal user identifiers, said user-specific entitlement associated with said packaged unique universal identifier (Wood col. 13 lines 28-36).

As per claim 30, Cohen, Weissman, Wood, and Johnson teach all the subject matter as described above. In addition Weissman teaches the computer readable medium further operable, when executed on a computer processor, to perform the step of requesting a user credential (Weissman

Page 6 par. 0032, and page. 7 par. 0036). The rational for combining are the same as claim 28

above.

Claim Rejections - 35 USC § 102

6.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7.   Claims 1, 12, 18, 23 and 28 are again rejected under 35 U.S.C. 102(e) as being

anticipated by Saito et al. (Saito, US 6,275,941 B1).

Regarding claim 1, Saito discloses a method for authenticating and authorizing a user of an

electronic device in communication with a network (**col. 1 lines 5-10**), comprising:

receiving a user request from a user of an electronic device in communication with a

network (col. 3 lines 8-11; *client requesting authentication to authentication server via network*);

searching for information relating to said user in a repository of user information, said

searching based at least partially on said user request and a login identity supplied by said user

(col. 6 lines 59-col. 7 lines 4 and fig. 4; *searching for relating info. in the storage based on user*

ID);

retrieving, from the repository of user information, a unique universal user identifier

representing said user upon locating said information of said user (abstract, and col. 6 lines 59-

col. 7 lines 4; *authentication server retrieving **common integrated certificate/unique universal ID** based on security information retrieved*);

storing at least said unique universal user identifier in a data packet (col. 9 lines 24-31; *transmitting common integrated certificate to user*);

sending said data packet to a storage device such that said data packet is transmittable to electronic devices in communication with said network when said user attempts to access a resource within said network (col. 9 lines 29-35; *client storage unit storing the received common integrated certificate*); and

retrieving an authorization datum associated with said user, based at least partially on said unique universal user identifier, from said resource (fig. 6 element 610; *application server retrieving confirmation of integrated certificate information based on user ID and password*).

Regarding claim 12, Saito discloses a method for accessing a plurality of resources having different authorization requirements, comprising:

accessing, via an electronic device, a network comprising a plurality of resources (abstract; *a client server access plurality of application servers/resources via networks*);

providing identifying data to said network (col. 2 lines 1-3; *user providing user ID and password*);

retrieving, in response to the identifying data, a unique universal user identifier corresponding to said user from a repository of unique universal user identifiers (abstract, and col. 6 lines 59-col. 7 lines 4; *authentication server retrieving **common integrated certificate/unique universal ID** based on security information retrieved*);

storing said unique universal user identifier on a storage device, said unique universal

user identifier indicating said user is authenticated (col. 9 lines 29-35; *client storage unit storing*

the received common integrated certificate if user is authentic); and

accessing one of said plurality of resources, wherein said unique universal user identifier

is transmitted to said one of said plurality of resources to identify said user such that said user

can access authorized resources without providing additional identifying information and said

user is denied access to unauthorized resources (abstract and col. 5 lines 50-55).

Regarding claim 18, Saito discloses a method of user authentication and authorization,

comprising:

accessing a repository containing a plurality of unique universal user identifiers, each of

said unique universal user identifiers being unique to a user (abstract, and col. 5 lines 33-67;

plurality of users common/unique integrated certificates stored on authentication storage unite is

accessed and provided to users and/or application servers to provide single sign-on service from

different application servers to users);

retrieving one of said unique universal user identifiers from said repository (abstract, and

col. 6 lines 59-col. 7 lines 4; *authentication server retrieving common integrated*

certificate/unique universal ID based on security information retrieved);

storing said unique universal user identifier in a data packet readable by an electronic

device (col. 9 lines 24-31; *transmitting common integrated certificate to user*);

transmitting said data packet to a storage device coupled to said electronic device (col. 9

lines 29-35; *client storage unit storing the received common integrated certificate*); and

making said data packet available to a resource configured within an enterprise network

to authorize said user (col. 1 lines 61-65; *integrated certificate is available to application servers*

when users are authenticated and authorized).

Regarding claim 23, Saito discloses a system for user authentication and authorization,

comprising:

a repository containing a plurality of unique universal user identifiers, each unique

universal user identifier being unique to a user (abstract, and col. 5 lines 33-67; *plurality of users*

common/unique integrated certificates stored on authentication storage unite is accessed and

provided to users and/or application servers to provide single sign-on service from different

application servers to users);

a first software tool operable to receive user login information, access said repository,

retrieve a unique universal user identifier relating to said user, and transmit said unique universal

user identifier to an electronic storage device suitable for storing said unique universal user

identifier in a data packet for transmission to resources within a network (abstract, and col. 6

lines 59-col. 7 lines 4; *authentication server retrieving **common integrated certificate/unique***

***universal ID** based on security information retrieved*); and

a second software tool suitable for receiving said data packet and locating authorization

datum of said user (col. 7 lines 40-67; *application server*).

Regarding claim 28, Saito discloses a computer-readable medium encoded with logic operable,

when executed on a computer processor, to perform the steps comprising:

receiving a user request from a user of an electronic device (col. 7 lines 5-24);

searching for a user credential corresponding to said user in an authentication database

(col. 6 lines 59-col. 7 lines 4 and fig. 4; *searching for relating info. in the storage based on user*

ID);

locating said user credential in said authentication database (abstract, and col. 6 lines 59-

col. 7 lines 4; *authentication server locating common integrated certificate/unique universal ID*

based on security information retrieved);

retrieving a unique universal user identifier representing said user upon locating said user

credential (abstract, and col. 6 lines 59-col. 7 lines 4; *authentication server retrieving common*

integrated certificate/unique universal ID based on security information retrieved);

packaging said unique universal user identifier in a data packet (col. 9 lines 24-31;

transmitting common integrated certificate to user); and

transmitting said data packet to said electronic device such that said data packet is

transmittable to electronic devices in communication with a network when said user attempts to

access a resource within said network such that said user can access authorized resources without

providing additional identifying information (abstract and col. 5 lines 50-55).

Conclusion

8.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure. US 6,836,799 B1: *Philyaw et al. discloses a user providing information like serial*

number, name, address, job, income level, general family history, demographic information

and more and generating unique identification/unique ID based on user information provided

i.e. generating a unique universal identifier is very well known in the art.

9.   For more prior art of record see form PTO 892 attached.

10.   Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this
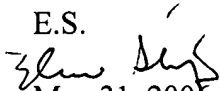
final action.

11.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867.

The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.

May 31, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100